DETAILED ACTION

1. This action is in response to original action filed on June 21, 2006. Claims 1-18 are pending.

Priority

Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(d). This application is a 371 of PCT/IB04/52793 filed on 12/13/2004 and further claims foreign priority to EUROPEAN PATENT OFFICE (EPO) 03104970.3 filed on 12/24/2003.

Claim Objections

2. Claims 1, 14-16, and 18 are objected to because of the following informalities: Claim limitations contain numeric reference such as, **"user device (110,721)"**. Applicant is advised to delete all numeric reference. Appropriate correction is required.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

3. Claim 17 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim 17 is directed to a signal for is non-statutory subject matter. Applicant's recital of "signal" includes physical but transitory

forms of signal transmission, such as radio broadcasts, electrical signals, and light pulses through fiber optic cable, that do not fall into the four statutory class defined by 35 U.S.C. 101.

Applicant is advised to amend claim 17 such that the term "signal" is deleted and further properly reads, "a method according to claim 1 comprising data communication for transmitting a certificate", to overcome 101 rejection.

4. Claim 18 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Claim is directed to a computer product for which is non-statutory subject matter. The recitation of the intended use of the computer program product on a computer having a computer readable medium does not require the computer program product to be encoded on a computer-readable medium. Accordingly, the scope of the claims includes the computer program product by itself, which is function descriptive material and does not fall into at least one of the four statutory classes defined by 35 U.S.C. 101. The computer program product, only imparts functionality when employed as a computer component, such as when a computer program is recorded on a computer readable medium.

Applicant is advised to amend claim 18 to read, " A computer readable medium comprising instructions executing on a processor to perform implementing at least one protocol side of at least one of: - the certificate issuing protocol, - the certificate re-issuing protocol, the certificate verification protocol", to overcome 101 rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

5. Claims 1-18 are rejected under 35 U.S.C. 102(b) as being anticipated by Saito et al. (NPL "Privacy Enhanced Access Control by SPKI" and Saito hereinafter).

6. As to claim 1, Saito teaches a **method of preserving privacy for a user while enabling the user controlled access to data, the user being represented by a user device (110,721) and identified by a user identity** (i.e., … teaches a client identified by a certificate [par. I, introduction]), **the method using at least one certificate that associates data access rights with the user identity** (i.e., … teaches a certificate for access control [par. I, introduction]), **where the certificate conceals the user identity** (i.e., … teaches the use of a certificate to conceal identity of client [abstract]), **the certificate comprises publicly available solution information P** (i.e., … teaches the certificate containing public key [par. I, Introduction], **and a concealed secret S' is publicly available** (i.e., … teaches public key corresponding to a private key [par. I, Introduction]), **the method further comprises at least one of - a certificate verification process (120,420) between the user device and a verifier device (111,701)** (i.e., ... teaches client submits a certificate to a server. … teaches the server verifies [par. III, pg. 305, (4) Exercise]) , **- a certificate issuing process (220,520,620)**

between the user certificate device and an issuing device (211,711) (i.e., .. teaches a issuing agent for creating and issuing a certificate to a client [pg. 304, (3) Issue]), **and a certificate re-issuing process (320) between the user device and the issuing device** (i.e., … teaches a certificate re-issue process [pg. 306, (B) Security of SPKI…]), **wherein the certificate verification process comprises the steps of - the user device obtaining the concealed secret S' corresponding to the certificate, 20 - the user device retrieving the secret S from the concealed secret S', - the verifier device obtaining the solution information P from the certificate** (i.e., … teaches verification process [pg. 305, col. 1, (4) Exercises] , - **the user device proving to the verifier device that it knows the secret S without the verifier device learning the secret S or the user identity** [abstract], **wherein the certificate issuing process comprises the steps of: 25 - generating a secret S and a solution information P** (i.e., … teaches a generating a secret [pg. 304, (3) Issue]), **- concealing the secret S into a concealed secret S', - the issuing device issuing a certificate comprising at least the solution information** P [fig. 5], **where the certificate re-issuing process comprises the steps of - the user device obtaining the concealed secret S' corresponding to the certificate** (i.e., … teaches a certificate re-issue process [pg. 306, (B) Security of SPKI…]), **the user device retrieving the secret S from the concealed secret S', the issuing device obtaining the solution information P from the certificate** [fig. 5], 5 **the user device proving to the issuing device that it knows the secret S without the issuing verifier device learning the secret S or the user identity** [abstract], **generating a new secret S and new solution information P2,**

concealing the secret S into a concealed secret S ' , - the issuing device issuing a new certificate comprising at least the new solution information t'2 [fig. 4].

7. As to claim 2, Saito teaches a **method where the certificate comprises publicly available concealed secret S'** (i.e.., user identity) (i.e., ... teaches ID (i.e., user identity) certificate binds the an identity (i.e., secret) and public key [pg. 301, par. I, Introduction, col. 2[]).

8. As to claim 3, Saito teaches a **method where the secret S is encrypted with the user's public key to generate the concealed secret S'** (i.e., … teaches encrypting with user public key [pg. 306, col. 1, (B) Security of SPKI-based Access Control]).

9. As to claim 4, Saito teaches a **method where the solution information P and the secret S are members of Zn*** (i.e., ... teaches public key infrastructure (P(I), P(S), TRUE, (,filel, file2), (Z/Jan/2000) [pg. 302, col. 2, (B.1) SPKI Certificate Format), **and the solution information P is the square of S** [pg. 303, col. 1, (b.2) Reduction Rule}.

10. As to claim 5, Saito teaches a **method where the concealed secret S' comprises random information RAN** [pg. 304, col. 1, (4) Exercise].

11. As to claim 6, Saito teaches a **method where the verifier device verifies that the 25 user device has knowledge of the secret S using a zero-knowledge protocol** (i.e., ... teaches the verifier checks the properness of the certificate submitted by the client [pg. 305, (A.1) Authorized Server].

12. As to claim 7, Saito teaches a **method where the communication during the issuing process is protected using symmetric key encryption** (i.e., ... teaches a public key and corresponding private key [pg. 301, par. I, Introduction, col. 2]).

13. As to claim 8, Saito teaches a **method according where in the issuing process the secret S and the solution information P** (i.e., .request) **is generated by the user device** (i.e., ... teaches a issuing process of a certificate by a issuing agent [pg. 302, col. 1, (A) Network Model] … further teaches a client submitting to issuing agent a request to the certificate [pg. 305, col. 2, (A2) Issuing Agent).

14. As to claim 9, Saito teaches a **method where the certificate is an authorization certificate** (i.e., … teaches a authorization certificate for access control [pg. 301, par. I, Introduction]).

15. As to claim 10, Saito teaches a **method where the certificate is a domain certificate** (i.e., … teaches a attribute certificate [pg. 301, par. I, Introduction]).

16. As to claim 11, Saito teaches a **method where the concealed secret S' in the domain certificate comprises the secret S, encrypted with the secret domain key** (i.e., ... teaches modification of the certificate [pg. 306, col. 1, (B) Security of SPKI-based Access Control]).

17. As to claim 12, Saito teaches a **method where the concealed secret S'** (i.e., ID certificate) **comprises the secret S, multiplied with cr_id** (i.e., … teaches the binding of an identity and a public key [pg. 301, col. 2, par. I, Introduction]) .

18. As to claim 13, Saito teaches a **method where the certificate comprises two secrets, of which the knowledge** (i.e. certificate) **prove by a user device gives different access levels** (i.e., … teaches a client initiates access to a server. … certificate of user is validated [pg. 305, (A.1) Authorized Server]).

19. As to claim 14, Saito teaches a **user device (110,721) being arranged for issuing a certificate** (i.e., … teaches a issuing agent [fig. 5]), **comprising: receiving means (727) for receiving process information (**i.e., … teaches retrieving from issuing agent [pg. 305, (A.3) Client}), **15 computing means (722)** (i.e., … teaches a validation processing [pg. 305, (A.3) Client]), **comprising processing (723), encryption/decryption (725) and storing means (724)** (i.e., … teaches encryption and decryption [pg. 305, (A.3) Client] … file storage [pg. 305, (A.3) Client]), **for engaging in at least one of the certificate verification process** (i.e., … teaches

verifying the validity of the certificate [pg. 305, (A.3) Client]), **the certificate issuing process** [fig. 5], **and certificate re-issuing process** (i.e., … teaches a certificate re-issue process [pg. 306, (B) Security of SPKI…]), **and - transmitting means (726) for transmitting process information** [fig. 5].

20. As to claim 15, Saito teaches a **verifier device (111,701) being arranged for verifying a certificate comprising: - receiving means (707) for receiving process information** [pg. 305, (A.1) Authorised Server], **- computing means (702), comprising processing (703)** [pg. 305, (A.1) Authorised Server], **encryption/decryption (705) and storing means (704)** (i.e., … teaches the server maintaining the client public key and possessing the ability to use cryptographic processing [pg. 306, (B) Modification of Certificate]), **for engaging in the certificate verification process** (i.e., … teaches certificate verification [pg. 305, (A.1) Authorised Server]), **and 25 - transmitting means (706) for transmitting process information** [fig. 5].

21. As to claim 16, Saito teaches a **issuing device (211,711) being arranged for issuing a certificate comprising: - receiving means (717) for receiving process information** [fig. 5], **30 - computing means (712)** (i.e., ... teaches the ability to perform authentication [pg. 305, (A.2) Issuing agent], **comprising processing (7 13), encryption/decryption (715) and storing means (714)** (i.e., … teaches encrypt and decrypt [pg, 305, (A.3) Client] ... further teaches storing map to public key [pg. 305, (A.2) Issuing]), **for engaging in at least one of the certificate issuing process and**

certificate re-issuing process (i.e., … teaches a certificate re-issue process [pg. 306, (B) Security of SPKI…]), **and - transmitting means (716) for transmitting process information** [fig. 5].

22. As to claim 17, Saito teaches a **signal carrying at least part of a certificate as used in the method according to claim 1** [fig. 5].

23. As to claim 18, Saito teaches a **computer program product (732) carrying computer executable instructions comprising a computer readable medium, having thereon computer program code means, to make a computer execute, when said computer program code means is loaded in the computer, implementing at least one protocol side of at least one of: - the certificate issuing protocol** (i.e., … teaches certificate issuing [pg. 304, (3) Issue]), **- the certificate re-issuing protocol** (i.e., … teaches a certificate re-issue process [pg. 306, (B) Security of SPKI…]), **the certificate verification protocol** (i.e., ... teaches client submits a certificate to a server. … teaches the server verifies [par. III, pg. 305, (4) Exercise] and [fig. 5]).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BRYAN WRIGHT whose telephone number is (571)270-3826. The examiner can normally be reached on 8:30 am - 5:30 pm Monday -Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, AYAZ Sheikh can be reached on (571)272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BRYAN WRIGHT/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431